Fix (RFI - LFI - XSS)
عمل رقعة امنية لعدة ثغرات

تأليف : Ghost Hacker
المدونة : http://gh05th4ck.wordpress.com

في هذا المقال سنتطرق الى تأمين تطبيقات البي اتش بي من عدة ثغرات الامنية .
سوف اشرح تأمين التطبيقات من ثغرات الـ Cross-site scripting او الـ XSS
و ثغرات الـ Remote File Include و ثغرات الـ Local File Include .
اما بخصوص التأمين من الـ SQL injection
سنتطرق لذلك في مقال لأحق بأذن الله !

اولاً : ثغرات الـ Remote File Include
يعمل هذا النوع على تمكين المهاجم من ادراج ملف خارجي الى ملفات الموقع بشكل غير شرعي .
يقوم المهاجم على الاغلب من خلال هذه الثغرة بأدراج ملف phpshell
يستطيع من خلاله التلاعب بالموقع وقد يصل الى التلاعب بالخادم كاملا !

كيف يتم اصابة البرامج بهذه الثغرة ؟
تتم الاصابة عن طريق استخدام الدوال التالية بالبرنامج
(Include و Include_once و Require و Require_once)
متبوعة بالـ $ (متغير) . ناخذ مثالا لكود بسيط مصاب

```
<?php
$ghost = $_GET['hacked'];
include ($ghost);
?>
```

بالسطر الاول من الكود تم وضع متغير بأسم ghost واعطائه القيمة التالية "hacked"
وفي السطر الثاني من الكود تم استخدام الدالة include
واستخدام علامة الـ $ قبل اسم المتغير ghost من بين الاقواس .

كيف يمكنني تأمين البرامج من هذا النوع ؟
التأمين او الترقيع يكون عن طريق تعريف المتغير المصاب لـ (./)
مثلا ترقيع الكود السابق من الثغرة يكون بهذا الشكل

```
<?php
$ghost = $_GET['hacked'];
$ghost = "./";
include ($ghost);
?>
```

مع استبدال ghost بأسم المتغير الملحق بالـ $.

ثانيا : ثغرات الـ Local File Include
يعمل هذا النوع على تمكين المهاجم من قراءة اكواد ملفات الموقع المصاب .

كيف يتم اصابة البرامج بهذه الثغرة ؟
تتم الاصابة بهذا النوع من الثغرات عن طريق بعض الدوال ومنها
(file و readfile و show_source و fread)
مثال على كود مصاب

```
<?php
readfile($hacked);
?>
```

نلاحظ استخدام الدالة readfile والـ $ مسبوق بـ hacked بداخل الاقواس .

كيف يمكنني تأمين البرامج من هذا النوع ؟
لتأمين او الترقيع يكون عن طريق تعريف المتغير المصاب لـ (./)
كما ثغرات الريموت فايل انكلود
مثال على نفس الكود المصاب اعلاه

```
<?php
$hacked = "./";
readfile($hacked);
?>
```

مع استبدال hacked بأسم المتغير الملحق بالـ $.

ثالثاً : ثغرات الـ XSS
يعمل هذا النوع على تمكين المهاجم من زرع اكواد
جافا سيكربت و HTML بالملف المصاب .
ينتج عن ذلك في معظم الاوقات تمكن المهاجم من سحب كوكيز ادمن الموقع عن طريق ملف Log !
يختلف هذا النوع عن باقي الثغرات فأن تنفيذه لأيكون على الموقع نفسه يكون على مستخدمين الموقع .

كيف يتم اصابة البرامج بهذه الثغرة ؟
تتم الاصابة بهذا النوع من الثغرات غالبا عن طريق المربعات (search)
كمربع البحث الموجود ببعض برامج البي اتش بي .
مثال على كود مصاب

```
<?php
print $_GET['hacked'];
?>
```

كيف يمكنني تأمين البرامج من هذا النوع ؟
التأمين او الترقيع يكون عن طريق الدوال التالية
(htmlentities or htmlspecialchars) .
يكون ترقيع الكود اعلاه بهذا الشكل

```
<?php
print htmlspecialchars($_GET['hacked']);
?>
```

نلاحظ اننا في عملية الترقيع وضعنا الدالة htmlspecialchars بعد print
واضفنا قوسين حول الـ $_GET .
وبهذا الشكل لن يتم تنفيذ استغلال الثغرة وسيتم عرضه بالصفحة فقط لأغير !

(المقال عبارة عن مجهود شخصي ارجو ذكر المصدر عن النقل)

BY GHOST HACKER - http://gh05th4ck.wordpress.com
ghost-r00t@windowslive.com